Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Saturday, September 08, 2007

Partial and total orders

From Advances in Distributed Security:

> A basic issue of security and fault tolerance that must be resolved is the secure determination of which order events occured in. If a contract specifies a deadline and it goes down to the wire, how can a relying party or third party adjudicator determine whether the deadline was met? The outcome itself, and its fairness, may rest on fairly deciding who came first. If Alice tries to double-spend a piece of digital cash [C82], only the recipient who checks with the bank first is entitled to its value. But if the bank servers are replicated, which of the two recipients Bob or Charles checked with the bank first? In the case of a replicated property title service [S98] we have a similar problem -- if Alice transfers her title to two other owners, which new owner actually received the deed? If property is homesteaded on a first-come first-serve basis, which of two or more "land rushers" competing for a lucrative parcel is entitled to the land?
> **Lamport (Causal) Order**
> Imagine a network where computers don't know how to keep time very well -- they are always getting out of synchronization. (Alas, all you have to really think of here is the actual Internet with PCs). Such a network, called an *asynchronous* network, lacks an accurate and secure global clock time by which computers can determine the order in which events, which might be messages sent or instructions executed on a particular local machine, have happened. Lamport [L78] was among the first to tackle the problem of how to determine the order of events in such a network.
>
> A partial order means that we know in what order some of the elements are, but we aren't sure about some of the others, or some of the others may be equal. An example is the "less than or equal to" relationship among a group of integers, some of which can repeat. Some of the integers we know are less than some others, but an integer paired with itself is equal. A total order, on the other hand, is like the "less than" relationship among unique integers -- we can always tell when one integer is less than another -- there is no ambiguity left. In the case of events, a partial order means for some pairs of events we know whether one occured before another, and for some others we don't know. We use the same symbols as we would use for the analogous case of the integers, so that "x <= y" means "x either occured before y or we don't know whether it occured before or after y". In a total of events, we know for any two events which one happened first. We write "x < y" meaning "x occured before y."
>
> Lamport's answer to the event ordering problem was to show that parties (or, we use the terms equivalently here, nodes on the network) can agree on a partial order of events based on causal relationships between these events -- or at least the subset of events where we can determine that causation could occur. On a network, parties influence each other by

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

talking to each other -- in other words, by sending each other messages. Lamport used these messages as the basic building block for constructing his partial order, according to the following rules:

- 1. If an event is local to node P, every nonfaulty node agrees on P's opinion of it.
- 2. Every correct node agrees that every message was sent before it was received.
- 3. If we agree that event A occured before event B and that event B occured before event C, then we agree that event A occured before event C. In other words, this partial order is transitive.

Breaking Ties -- Creating a Fair Total Order
The partial order leaves us with the need to agree on how to break ties -- how to resolve the ambiguities where we can't agree which event took place first -- and thus create a total order of events. We want to do so in a way that is *fair*, in other words, in a way that cannot be manipulated to the advantage of any particular party.

An unfair way to create a total order would be to impose a certain predictable rule for breaking ties. For example, we could decide on a total order for the processes and break ties in the causal order by referring to this total order.

However, such a procedure creates a bias that may, depending on the application, favor certain servers over others, and therefore allow those servers to favor certain clients over others.

One way to break ties fairly is have the participants toss fair coins -- in other words, generate random numbers in a way that cannot be manipulated and then assign those random numbers to events. There are several ways to toss fair coins over a network and we describe one such way below.

Another way to break ties fairly is to have the participants agree to a global clock time that is more accurate than the message delays faced by those who would manipulate timing in favor of some party. This entails using a network with very predictable message lag for the clock synchronization protocol and a less predictable one for the other services.

More here.

Posted by Nick Szabo at 3:39 PM

3 comments:

blastomere said...

Although you are correct that "less than or equal" and Lamport's "time of arrival" are both partial orders, and both can be represented in abstract algebra terms by "<=", once we get more concrete the "=" has a very different meaning between the two cases. In the first it denotes equality whereas in the second it denotes ignorance.

7:28 PM

Anonymous said...

Also, your definition of "total order" is just wrong. See

http://en.wikipedia.org/wiki/Total_order

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ▼ 2007 (47)
  - ► December (1)
  - ► October (2)
  - ▼ September (8)
    - Secure time broadcast
    - Real options analysis for space projects
    - Tamper evident numbers
    - Mining the vasty deep (iii)
    - Partial and total orders
    - Institutional changes prerequisite to the industri...
    - Secure property titles
    - Bilinear group cryptography
  - ► August (10)
  - ► July (4)
  - ► June (4)
  - ► May (8)
  - ► April (1)
  - ► March (2)
  - ► February (4)
  - ► January (3)
- ► 2006 (130)
- ► 2005 (44)

or
http://planetmath.org/encyclopedia/TotalOrder.html

or any math book.

That paragraph needs to be completely rewritten.

10:59 AM

nick said...

What I wrote is completely consistent with those definitions. What is your real beef, "anonymous"?

2:03 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.